CLAIMS

What is claimed is:

1. A method for managing access to messages in a network, the method comprising the computer-implemented steps of:
receiving, from a first node in the network, a request for both a message identifier that uniquely identifies the message and a key that may be used to encode the message;
generating, in response to receiving the request, both the message identifier and the key;
providing both the message identifier and the key to the first node to allow the message to be encoded with the key to generate an encoded message;
receiving, from a second node in the network, a request for the key;
providing the key to the second node to allow the encoded message to be decoded and the message to be retrieved using the key; and
managing access to the key based upon key policy criteria.

2. A method as recited in Claim 1, wherein managing access to the key based upon key policy criteria includes deleting the key based upon the key policy criteria.

3. A method as recited in Claim 1, wherein managing access to the key based upon key policy criteria includes only providing the key to authorized entities in accordance with the key policy criteria.

4. A method as recited in Claim 1, wherein the steps are performed at a third node in the network that is different from the first and second node.

5. A method as recited in Claim 4, wherein the steps are performed by a key server executing at the third node.

6. A method as recited in Claim 1, further comprising verifying whether the first node is authorized to obtain the key.

7. A method as recited in Claim 1, wherein the request from the second node for the key specifies the message identifier, and the method further comprises verifying that the second node is authorized to receive the key.

8. A method as recited in Claim 1, further comprising generating and storing data that indicates that the key was provided to the first node or the second node.

9. A method as recited in Claim 1, further comprising generating and storing data that indicates that the encoded message was decoded at the second node using the key.

10. A method as recited in Claim 6, further comprising generating and storing data that indicates that the retrieved message was stored.

11. A method as recited in Claim 1, wherein the key policy criteria are managed at a third node in the network that is different than the first and second nodes.

12. A method as recited in Claim 1, wherein the key policy criteria include one or more of expiration date criteria, subject matter criteria and node identification criteria.

13. A method as recited in Claim 1, wherein the key policy criteria are dynamically changed over time.

14. A method as recited in Claim 1, further comprising generating meta data that specifies an attribute of the message, and wherein the step of deleting the key

based upon key policy criteria includes deleting the key by applying the key policy criteria to the meta data.

15. A method as recited in Claim 1, further comprising after the key is deleted and the next time the second node communicates with the network, instructing the second node to delete the message retrieved from the encoded message using the key.

16. A method as recited in Claim 1, further comprising providing location data to the second node that uniquely identifies a location where the key is maintained.

17. A method as recited in Claim 1, further comprising:
receiving and storing one or more encoded messages at the second node,
requesting, receiving, and storing at the second node, one or more keys, wherein each of the keys is associated with one of the encoded messages that are stored at the second node,
decoupling the second node from the network, and
decoding the encoded messages based on the keys.

18. A method as recited in Claim 1, further comprising:
generating a digital signature of the message and storing the digital signature in association with the message, and
providing the digital signature to the second node to enable the second node to validate the message.

19. A method as recited in Claim 1, further comprising:
receiving a request for a second message identifier and a second key,
encoding the encoded message using the second key to generate a twice-encoded message, and

communicating the twice-encoded message to a third node in the network.

20. A method as recited in Claim 19, wherein
the message identifier is included in the encoded message, and
the method further comprises
extracting the message identifier from the encoded message prior to encoding the encoded message using the second key, and
appending both the first message identifier and the second message identifier to the twice-encoded message prior to communicating the twice-encoded message to the third node.

21. A method as recited in Claim 1, further comprising:
extracting a second message identifier from a twice-encoded message,
receiving a request for a second key for the twice-encoded message,
providing the second key for the twice-encoded message,
decoding the twice-encoded message using the second key to recover the encoded message,
extracting the first message identifier from the encoded message,
receiving a request for the first key to decode the encoded message,
providing the first key to allow decoding of the encoded message, and
decoding the encoded message using the first key to recover the message.

22. A method as recited in Claim 1, further comprising:
extracting a first message identifier and a second message identifier from a twice-encoded message,
receiving a request for the first key and a second key for the twice-encoded message,
providing the first key and the second key to allow decoding of the twice-encoded message,

decoding the twice-encoded message using the second key to recover the encoded message, and

decoding the encoded message using the first key to recover the message.

23. A computer-readable medium for managing access to messages in a network, the computer-readable medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving, from a first node in the network, both a request for a message identifier that uniquely identifies the message and a key that may be used to encode the message;

generating, in response to receiving the request, both the message identifier and the key;

providing both the message identifier and the key to the first node to allow the message to be encoded with the key to generate an encoded message;

receiving, from a second node in the network, a request for the key;

providing the key to the second node to allow the encoded message to be decoded and the message to be retrieved using the key; and

managing access to the key based upon key policy criteria.

24. A computer-readable medium as recited in Claim 23, wherein managing access to the key based upon key policy criteria includes deleting the key based upon the key policy criteria.

25. A computer-readable medium as recited in Claim 23, wherein managing access to the key based upon key policy criteria includes only providing the key to authorized entities in accordance with the key policy criteria.

26. A computer-readable medium as recited in Claim 23, wherein the steps are performed at a third node in the network that is different from the first and second node.

27. A computer-readable medium as recited in Claim 26, wherein the steps are performed by a key server executing at the third node.

28. A computer-readable medium as recited in Claim 23, further comprising one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of verifying whether the first node is authorized to obtain the key.

29. A computer-readable medium as recited in Claim 23, wherein:
the request from the second node for the key specifies the message identifier, and
the computer-readable medium further comprises one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of verifying that the second node is authorized to receive the key.

30. A computer-readable medium as recited in Claim 23, further comprising one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of generating and storing data that indicates that the key was provided to the first node or the second node.

31. A computer-readable medium as recited in Claim 23, further comprising one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of generating and storing data that indicates that the encoded message was decoded at the second node using the key.

32. A computer-readable medium as recited in Claim 28, further comprising one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of generating and storing data that indicates that the retrieved message was stored.

33. A computer-readable medium as recited in Claim 23, wherein the key policy criteria are managed at a third node in the network that is different than the first and second nodes.

34. A computer-readable medium as recited in Claim 23, wherein the key policy criteria include one or more of expiration date criteria, subject matter criteria and node identification criteria.

35. A computer-readable medium as recited in Claim 23, wherein the key policy criteria are dynamically changed over time.

36. A computer-readable medium as recited in Claim 23, further comprising one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of generating meta data that specifies an attribute of the message, and wherein the step of deleting the key based upon key policy criteria includes deleting the key by applying the key policy criteria to the meta data.

37. A computer-readable medium as recited in Claim 23, further comprising one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of after the key is deleted and the next time the second node communicates with the network, instructing the second node to delete the message retrieved from the encoded message using the key.

38. A computer-readable medium as recited in Claim 23, further comprising one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of providing location data to the second node that uniquely identifies a location where the key is maintained.

39. A computer-readable medium as recited in Claim 23, further comprising one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:
receiving and storing one or more encoded messages at the second node,
requesting, receiving, and storing at the second node, one or more keys, wherein each of the keys is associated with one of the encoded messages that are stored at the second node,
decoupling the second node from the network, and
decoding the encoded messages based on the keys.

40. A computer-readable medium as recited in Claim 23, further comprising one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:
generating a digital signature of the message and storing the digital signature in association with the message, and
providing the digital signature to the second node to enable the second node to validate the message.

41. A computer-readable medium as recited in Claim 23, further comprising:
receiving a request for a second message identifier and a second key,
encoding the encoded message using the second key to generate a twice-encoded message, and

communicating the twice-encoded message to a third node in the network.

42. A computer-readable medium as recited in Claim 41, wherein the message identifier is included in the encoded message, and the method further comprises

extracting the message identifier from the encoded message prior to encoding the encoded message using the second key, and

appending both the first message identifier and the second message identifier to the twice-encoded message prior to communicating the twice-encoded message to the third node.

43. A computer-readable medium as recited in Claim 23, further comprising:

extracting a second message identifier from a twice-encoded message,

receiving a request for a second key for the twice-encoded message,

providing the second key for the twice-encoded message,

decoding the twice-encoded message using the second key to recover the encoded message,

extracting the first message identifier from the encoded message,

receiving a request for the first key to decode the encoded message,

providing the first key to allow decoding of the encoded message, and

decoding the encoded message using the first key to recover the message.

44. A computer-readable medium as recited in Claim 23, further comprising:

extracting a first message identifier and a second message identifier from a twice-encoded message,

receiving a request for the first key and a second key for the twice-encoded message,

providing the first key and the second key to allow decoding of the twice-encoded message,

decoding the twice-encoded message using the second key to recover the encoded message, and

decoding the encoded message using the first key to recover the message.

45. An apparatus for managing access to messages in a network, the apparatus comprising a memory carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving, from a first node in the network, both a request for a message identifier that uniquely identifies the message and a key that may be used to encode the message;

generating, in response to receiving the request, both the message identifier and the key;

providing both the message identifier and the key to the first node to allow the message to be encoded with the key to generate an encoded message;

receiving, from a second node in the network, a request for the key;

providing the key to the second node to allow the encoded message to be decoded and the message to be retrieved using the key; and

managing access to the key based upon key policy criteria.

46. An apparatus as recited in Claim 45, wherein managing access to the key based upon key policy criteria includes deleting the key based upon the key policy criteria.

47. An apparatus as recited in Claim 45, wherein managing access to the key based upon key policy criteria includes only providing the key to authorized entities in accordance with the key policy criteria.

48. An apparatus as recited in Claim 45, wherein the steps are performed at a third node in the network that is different from the first and second node.

49. An apparatus as recited in Claim 48, wherein the steps are performed by a key server executing at the third node.

50. An apparatus as recited in Claim 45, wherein the memory further comprises one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of verifying whether the first node is authorized to obtain the key.

51. An apparatus as recited in Claim 45, wherein:
the request from the second node for the key specifies the message identifier, and
the memory further comprises one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of verifying that the second node is authorized to receive the key.

52. An apparatus as recited in Claim 45, wherein the memory further comprises one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of generating and storing data that indicates that the key was provided to the first node or the second node.

53. An apparatus as recited in Claim 45, wherein the memory further comprises one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of generating and storing data that indicates that the encoded message was decoded at the second node using the key.

54. An apparatus as recited in Claim 50, wherein the memory further comprises one or more additional instructions which, when executed by the one or more processors,

cause the one or more processors to perform the step of generating and storing data that indicates that the retrieved message was stored.

55. An apparatus as recited in Claim 45, wherein the key policy criteria are managed at a third node in the network that is different than the first and second nodes.

56. An apparatus as recited in Claim 45, wherein the key policy criteria include one or more of expiration date criteria, subject matter criteria and node identification criteria.

57. An apparatus as recited in Claim 45, wherein the key policy criteria are dynamically changed over time.

58. An apparatus as recited in Claim 45, wherein the memory further comprises one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of generating meta data that specifies an attribute of the message, and wherein the step of deleting the key based upon key policy criteria includes deleting the key by applying the key policy criteria to the meta data.

59. An apparatus as recited in Claim 45, wherein the memory further comprises one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of after the key is deleted and the next time the second node communicates with the network, instructing the second node to delete the message retrieved from the encoded message using the key.

60. An apparatus as recited in Claim 45, wherein the memory further comprises one or more additional instructions which, when executed by the one or more processors,

cause the one or more processors to perform the step of providing location data to the second node that uniquely identifies a location where the key is maintained.

61. An apparatus as recited in Claim 45, wherein the memory further comprises one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:
receiving and storing one or more encoded messages at the second node,
requesting, receiving, and storing at the second node, one or more keys, wherein each of the keys is associated with one of the encoded messages that are stored at the second node,
decoupling the second node from the network, and
decoding the encoded messages based on the keys.

62. An apparatus as recited in Claim 45, wherein the memory further comprises one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:
generating a digital signature of the message and storing the digital signature in association with the message, and
providing the digital signature to the second node to enable the second node to validate the message.

63. An apparatus as recited in Claim 45, further comprising:
receiving a request for a second message identifier and a second key,
encoding the encoded message using the second key to generate a twice-encoded message, and
communicating the twice-encoded message to a third node in the network.

64. An apparatus as recited in Claim 63, wherein

the message identifier is included in the encoded message, and
the method further comprises
extracting the message identifier from the encoded message prior to encoding the encoded message using the second key, and
appending both the first message identifier and the second message identifier to the twice-encoded message prior to communicating the twice-encoded message to the third node.

65. An apparatus as recited in Claim 45, further comprising:
extracting a second message identifier from a twice-encoded message,
receiving a request for a second key for the twice-encoded message,
providing the second key for the twice-encoded message,
decoding the twice-encoded message using the second key to recover the encoded message,
extracting the first message identifier from the encoded message,
receiving a request for the first key to decode the encoded message,
providing the first key to allow decoding of the encoded message, and
decoding the encoded message using the first key to recover the message.

66. An apparatus as recited in Claim 45, further comprising:
extracting a first message identifier and a second message identifier from a twice-encoded message,
receiving a request for the first key and a second key for the twice-encoded message,
providing the first key and the second key to allow decoding of the twice-encoded message,
decoding the twice-encoded message using the second key to recover the encoded message, and
decoding the encoded message using the first key to recover the message.